TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

CONFIGURING THE TPM AND PROTECTING PRIVATE KEYS IN SNS FIREWALL CERTIFICATES

Product concerned: SNS 4.3.37 LTSB and higher 4.3 LTSB, SNS 4.8.7 and higher versions

Document last updated: June 10, 2025

Reference: sns-en-TPM_protection_technical_note

Table of contents

Change log

Date	Description
June 10, 2025	• Explanations regarding the symmetric key and PCRs added to the "How it works" section • Explanations regarding the symmetric key derivation mechanism on SNS 4.3 LTSB versions added to the "How it works" and "Initializing the TPM on SNS firewalls" sections • Explanations regarding the removal of protection on private keys, and regarding SNS firewall pools managed by an SMC server added to the "Managing protection on private keys in SNS firewall certificates" section • Explanations regarding the use of certificates with a private key that has been protected for VPN services on the SNS firewall added in the section "Using certificates with TPM-protected private keys" • New section "Appendix: points to note when updating SNS firewalls on which the TPM has been initialized" added
May 06, 2025	• New requirement regarding the activation of the Secure Boot feature added in the "Requirements" section • Information on the TPM administration password, symmetric key, PCRs, and TPM sealing added in the "How it works" section • Content relating to TPM initialization updated, and now has its own separate section in the document • Information regarding the verification of TPM status and TPM sealing added in the section "Managing the TPM on SNS firewalls" • Clarification regarding the verification of protection on a certificate's private key added in the section "Protecting private keys of certificates on SNS firewalls" • Explanations regarding the use of a backup certificate for the web administration interface added in the section "Using certificates with TPM-protected private keys" • Explanations regarding the calculation of the high availability quality factor when the Secure Boot feature is enabled added in the section "Explanations on usage when the TPM is initialized" • Contents of the "Troubleshooting" section enriched
December 13, 2024	• Explanations added regarding the initialization of the TPM in a high availability cluster

February 13, 2024	• Explanations regarding PCRs added to the section "Protecting private keys in firewall certificates with symmetric keys" • Changes to the description of the TPM orange status in the section "Checking whether the TPM is initialized" • Explanations on resetting the TPM added to the section "If you have forgotten the TPM password" • Explanation on the `force=on` token reworded in the section "Disabling the TPM" • The example *<CN>* changed to *<CERTNAME>* in the sections "Protecting the private key of a certificate that has already been added" and "Checking whether the private key in the SNS firewall's certificate is protected" • Information regarding the certification authority reworded in the "SSL VPN" section • Important information regarding the use of protected private keys added to the section "Communications with the SMC server" • Explanations on protecting the backup file with a password added to the section "Backing up a configuration"
January 18, 2024	• New document

Getting started

The trusted platform module (TPM) found on SNS firewalls offers hardware storage that increases the security of certificates stored on the SNS firewall.

The TPM-based security mechanism applies to some certificates, depending on the version installed on the SNS firewall.

This technical note provides details on:

- How the TPM functions,
- Initializing and configuring the TPM on SNS firewalls,
- Managing protection on private keys in SNS firewall certificates
- Using certificates with protected private keys in the an SNS firewall configuration,
- Important points to note when updating SNS firewalls on which the TPM has been initialized.

NOTE
To update the TPM version on an SNS firewall, refer to the technical note Updating the TPM version on SNS firewalls.

Requirements

This section sets out the requirements for initializing and configuring the TPM on an SNS firewall.

An SNS firewall equipped with a TPM

See the list of the relevant firewall models on the Stormshield website at Our Stormshield Network Security firewalls.

Secure Boot enabled on the SNS firewall

On SNS in 4.8.7 and higher versions, the integrity of the SNS firewall and its TPM will be compromised if Secure Boot is not enabled. We recommend that you enable it before initializing the TPM, or reseal the TPM.
Do note that a warning will be appear in the SNS firewall **Dashboard** if Secure Boot is disabled, and the TPM is initialized.

On SNS 4.3.37 LTSB and higher 4.3 LTSB versions, you are advised to enable Secure Boot on the SNS firewall, even though it is not mandatory.

NOTE
Secure Boot is enabled by default on some SNS firewall models. For more information on the models concerned, and on enabling Secure Boot, refer to the technical note Managing Secure Boot in SNS firewalls' UEFI.

Permissions to access the TPM

To initialize and configure the TPM, the administrator must hold the **TPM access (W)** privilege. Only the *admin* account can assign this privilege in **Configuration > System > Administrators**, **Administrators** tab, **Switch to advanced view** button.

Ability to access the CLI console on the SNS firewall

If you wish to perform any of the actions mentioned in this technical note from the SNS firewall's CLI console, go to **Configuration > System > CLI console** from the SNS firewall's web administration interface. For more information, refer to the section **CLI console** in the *SNS* v4.8 or v4.3 LTSB *user guide*, depending on the version used.

How it works

This section lists the certificates with private keys that can be protected by the TPM, and provides explanations on the TPM administration password, symmetric key and its derivation mechanism, PCRs, and the importance of having access to the TPM.

List of certificates with private keys that can be protected by the TPM

TPM protection applies to some certificates, depending on the SNS version installed.

Certificates used in the following cases with a private key that can be protected by the TPM	Compatible SNS versions	
	4.3.37 LTSB and higher 4.3 LTSB versions	4.8.7 and higher versions
IPsec VPN	✓	✓
SSL VPN	-	✓
SSL/TLS decryption (web administration interface and captive portal)	-	✓
Communications with the SMC server	-	✓
Sending of logs to a syslog server	-	✓
Internal LDAP	-	✓

TPM administration password

A TPM administration password has to be set during its initialization. In this technical note, it is referred to as "*TPM password*".

You will be asked to provide this password for certain maintenance operations, when modifying the BIOS, after certain software updates, or after the SNS firewall boot partition is changed.

With regard to the TPM password:

- It must comply with the password policy set on the SNS firewall,
- On SNS in 4.8.7 and higher versions, we recommend generating it randomly with a length of at least 64 characters. Due to a restriction on SNS 4.3.37 LTSB and higher 4.3 LTSB versions, its length must not exceed 32 characters.
- **It must be kept in a secure and protected location.**

IMPORTANT
If you misplace the TPM password, you will not be able to reinitialize it, and Stormshield is not in a position to recover the password. This scenario is described in the section Troubleshooting".

Symmetric keys

Introduction

A symmetric key is set during the initialization of the TPM and stored on the TPM. When the private key of a certificate is protected by the TPM, the key will be encrypted with a symmetric key.

Only the symmetric key will enable the encryption and decryption of a certificate's private key.

The symmetric key is sealed in the TPM, and access to it is strictly protected by the TPM password, and through a feature that reliably measures the status of the system, known as PCRs (platform configuration registers).

Symmetric key derivation mechanism

A symmetric key derivation mechanism (called *derivekey*) is used to generate the symmetric key from the TPM password when the TPM on an SNS firewall is initialized.

Firewalls have their own TPMs in high availability clusters. Two symmetric keys are therefore generated:

- A first symmetric key stored on the active firewall's TPM,
- A second symmetric key stored on the passive firewall's TPM.

To ensure service continuity when an SNS firewall cluster switches, the symmetric key that is stored on the active firewall has to be identical to the key that is stored on the passive firewall. When the TPM on both firewalls in the cluster is initialized, the derivation mechanism is automatically used, making it possible to generate the same symmetric key from the TPM password. As such, during a switch, each SNS firewall is able to decrypt the private keys.

This mechanism is also useful in an SNS firewall exchange (RMA) to restore configuration backups that contain protected private keys. Since only the symmetric key can be used to encrypt and decrypt protected private keys, the symmetric key that is stored on the new firewall must be identical to the one that was stored on the returned firewall.

Platform configuration registers

Introduction

The TPM is sealed by the PCRs based on a series of hashes. Their value is defined by a set of measures taken when the SNS firewall is starting up:

- BIOS version and options,
- Launched UEFI binaries (PCR 4),
- Partition table,
- Operating system,
- Connected hardware modules (such as network modules and USB devices),
- etc.

PCR hash values and access to the TPM

If PCR hash values change, access to the TPM module may be denied.

- On SNS in 4.8.7 and higher versions, access to the TPM will be denied if the value of the hashes on PCR 0 to 3 and 5 to 7 changes. The hash from PCR 4, which is linked to the SNS firewall startup sequence, is not taken into account in the TPM sealing policy. The Secure Boot feature monitors the integrity of the UEFI binaries in this boot sequence.
- On SNS in version 4.3.37 LTSB and higher 4.3 LTSB versions, access to the TPM will be denied if the value of the hashes on PCR 0 to 7 changes. This includes PCR 4, which is linked to the SNS firewall startup sequence. This hash can be modified after a version update that applies changes to the SNS firewall startup sequence.

When access to the TPM module is denied, the symmetric key can no longer be recovered, and protected private keys can no longer be decrypted without entering the TPM password.

To restore access to the TPM, ensure in advance that the change is legitimate. You must then reseal the TPM to update the value of PCR hashes. This procedure is described in the Sealing the TPM section.

IMPORTANT
If access to the TPM is denied, SNS firewall features that use certificates with protected private keys (VPN, those managed by an SMC server, etc.) will no longer function until access to the TPM is restored. Such blockages may occur, usually after an SNS firewall has been updated. This scenario is described in the section Appendix: points to note when updating SNS firewalls on which the TPM has been initialized.

Cases requiring the TPM to be resealed

The following cases require the TPM to be resealed:

- The TPM sealing policy was modified after a version update. Information is provided in the *SNS release notes* for this case.
- A BIOS option has been modified, for example if the SNS firewall's Secure Boot feature has been enabled or disabled.
- A physical maintenance operation has been conducted, for example if a USB device was plugged in or unplugged, or if a network module has been changed.
- The boot partition was modified and the SNS firewall was started on it. Do note that if the partition was selected in console mode during the interactive selection when the SNS firewall was started up, the TPM needs to be resealed after a second reboot.

Initializing the TPM on SNS firewalls

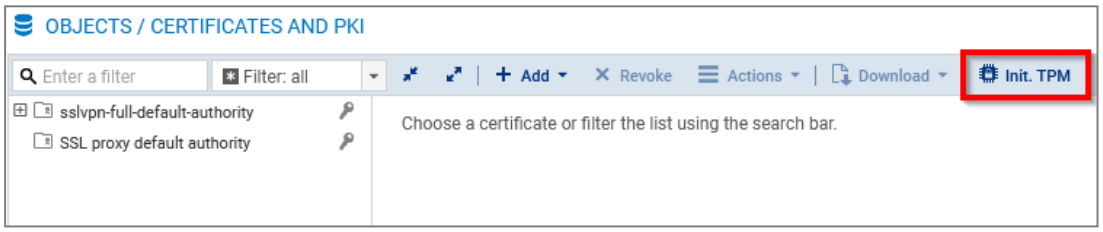
This section explains how to initialize the TPM on an SNS firewall or TPMs in an SNS firewall high availability cluster.

From the web administration interface

The initialization process varies according to the version installed on the SNS firewall.

SNS in 4.8.7 and higher versions

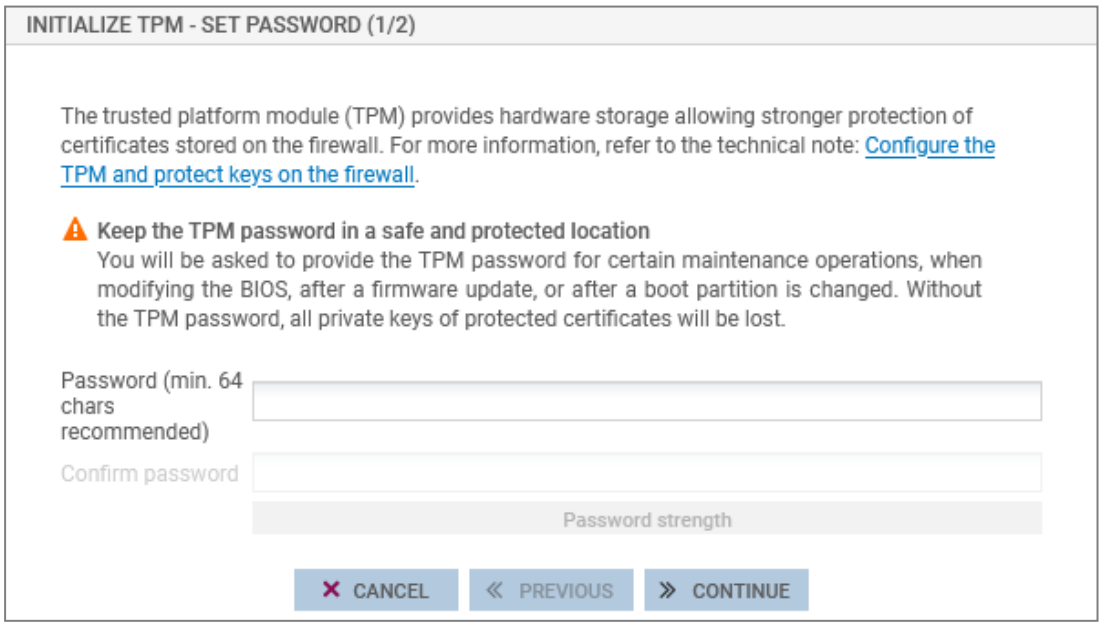
1. Go to **Configuration > Objects > Certificates and PKI**.
2. Click on **Init. TPM**.



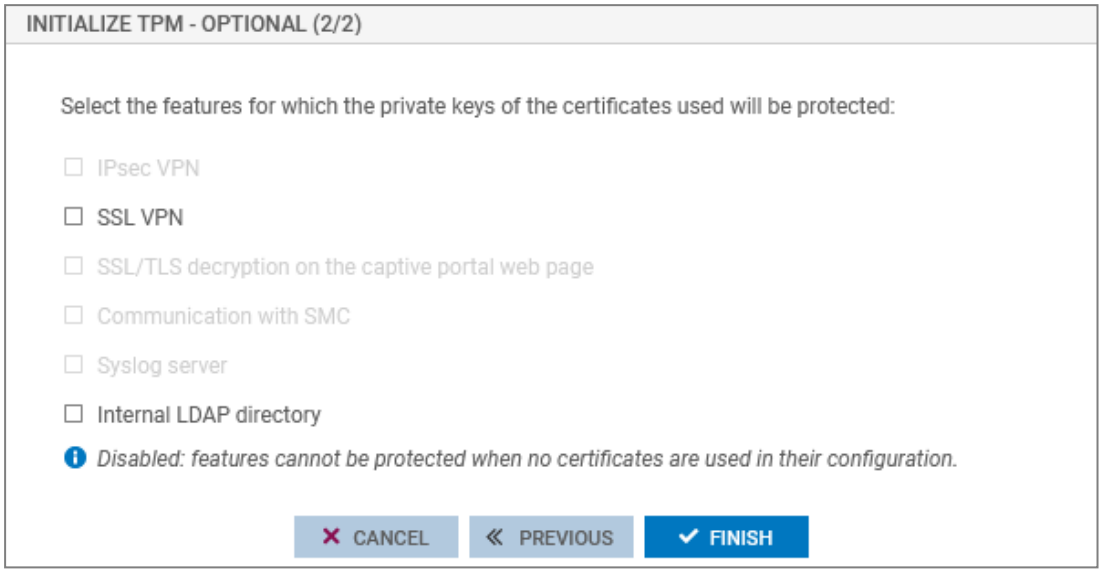
3. If Secure Boot has not been enabled, a warning will appear. You are advised to enable Secure Boot before initializing the TPM, but this can be done later.

> **IMPORTANT**
> As a reminder, the integrity of the SNS firewall and its TPM will be compromised if Secure Boot is not enabled.

4. In the **Set password** window, set the administration password of the TPM, by following the recommendations in the section TPM administration password, then click on **Continue**.



5. Select the features for which the private key of the certificate used will be protected. Features that do not use certificates in their configuration cannot be selected. You can also leave all checkboxes unchecked and protect private keys in SNS firewall certificates later.

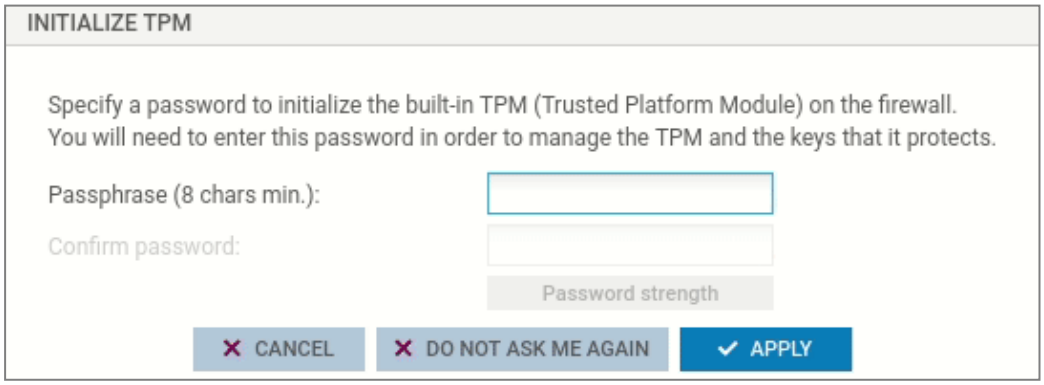


6. Click on **Finish**.

   The TPM is initialized and the mechanism that derives the symmetric key is used to generate the symmetric key, regardless of whether the SNS firewall is a member of a high availability cluster. If the SNS firewall is part of a high availability cluster, the TPM on the passive firewall will be automatically initialized.

SNS version 4.3.37 LTSB and higher 4.3 LTSB versions

1. Go to **Configuration > Objects > Certificates and PKI**.
2. In the window to initialize the TPM, set the administration password of the TPM, by following the recommendations in the section TPM administration password. If the window does not automatically appear, check whether the TPM has already been initialized, or initialize it from the CLI console.



3. Click on **Apply**.

   The TPM is initialized and the mechanism that derives the symmetric key is used to generate the symmetric key, regardless of whether the SNS firewall is a member of a high availability cluster. If the SNS firewall is part of a high availability cluster, the TPM on the passive firewall will be automatically initialized.

You then need to protect the private keys of certificates on the SNS firewall.

From the CLI console

1. Initialize the TPM on the SNS firewall with the command:
   ```
   SYSTEM TPM INIT tpmpassword=<password> derivekey=<on|off>
   ```
   - Replace `<password>` with the desired administration password of the TPM, by following the recommendations in the section TPM administration password,
   - If the SNS firewall is a member of a high availability cluster, enter `derivekey=on` to use the symmetric key derivation mechanism.
2. If the SNS firewall is part of a high availability cluster, initialize the TPM on the passive firewall with the command:
   ```
   HA TPMSYNC tpmpassword=<password>
   ```

You then need to protect the private keys of certificates on the SNS firewall.

When a high availability firewall cluster has not yet been created

The TPM has not yet been initialized on either firewall in the cluster

1. Configure the cluster (create the cluster and integrate the second SNS firewall).
2. Refer to the procedures above on initializing the TPM on SNS firewalls.

The TPM is already initialized on the future active firewall in the cluster

SNS in 4.8.7 and higher versions

1. Configure the cluster (create the cluster and integrate the second SNS firewall).
2. Log out of the SNS firewall's web administration interface and log back in.
3. A window will automatically appear, asking you to initialize the TPM on the passive firewall. Enter the TPM password in the relevant field.
4. Click on **OK**.

SNS version 4.3.37 LTSB and higher 4.3 LTSB versions

1. From a CLI console, renew the symmetric key on the active firewall with the command:
   ```
   SYSTEM TPM RENEW tpmpassword=<password> derivekey=on
   ```
   - Replace `<password>` with the TPM password,
   - As the firewall is a member of a high availability cluster, enter `derivekey=on` to use the symmetric key derivation mechanism.

   All TPM-protected private keys will be decrypted, then encrypted again with the new symmetric key derived from the TPM password.
2. Initialize the TPM on the passive firewall with the command:
   ```
   HA TPMSYNC tpmpassword=<password>
   ```

Managing the TPM on SNS firewalls

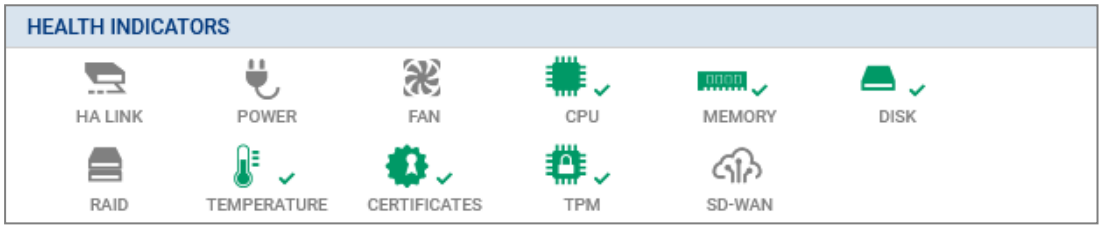
This section explains how to check the status of the TPM, change its administration password, seal it, and disable it.

Checking the status of the TPM

From the web administration interface

This use case is exclusive to SNS 4.8.7 and higher versions.

1. Go to **Monitoring** > **Dashboard**, in the **Health indicators** widget.



2. Check the color of the *TPM* health indicator icon to find out its status.

Icon	Description
None	The SNS firewall is not equipped with a TPM.
	The SNS firewall is equipped with a TPM, but it has not been initialized.
	The TPM is initialized, running and protects at least one private key.
	There are several possible statuses: • The TPM is initialized, but it not protecting any private key. By scrolling over the icon, the tooltip "*The TPM has been initialized, but is not in use*" confirms this status. • The TPM sealing policy has been changed. To apply it, reseal the TPM by following the Sealing the TPM procedure. By scrolling over the icon, the tooltip "*TPM sealing required in order to apply the new TPM sealing policy*" confirms this status.
	There are several possible statuses: • Tests on the TPM do not work (it no longer responds), • The TPM can no longer be accessed because the hash values of PCRs have changed. To refresh them, reseal the TPM by following the Sealing the TPM procedure. By scrolling over the icon, the tooltip "*TPM sealing required in order to recover access to the TPM*" confirms this status. • Secure Boot is disabled. A warning in the **Messages** widget in the **Dashboard** confirms that the feature is disabled. **IMPORTANT** As a reminder, the integrity of the SNS firewall and its TPM will be compromised if Secure Boot is not enabled.

From the CLI console

1. Show TPM monitoring information with the command:
```
MONITOR TPM
```
2. Check the result.

Token	Values/Description
ondisk_init	• 1: the TPM is initialized, • 0: the TPM has not been initialized. **NOTE** The other tokens below do not exist in SNS 4.3.37 LTSB and higher 4.3 LTSB versions.
secure_boot_enabled	• 1: Secure Boot is enabled, • 0: Secure Boot is disabled.
ondisk_pkeys_present	• 1: the TPM is protecting at least one private key, • 0: the TPM is not protecting any private keys.
pcr_access_status	• Good: the TPM can be accessed, no action is required. • Legacy: the TPM sealing policy has been changed. To apply it, reseal the TPM by following the Sealing the TPM procedure. A message confirms this status. • NO: the TPM can no longer be accessed because the hash values of PCRs have changed. To refresh them, reseal the TPM by following the Sealing the TPM procedure. A message confirms this status.
message	Specify information on the status of the TPM if necessary.

Changing the TPM administration password

From a CLI console, change the TPM administration password using the command:

```
SYSTEM TPM CHANGE currentpassword=<password> newpassword=<new_password>
```

- Replace `<password>` with the current TPM password,
- Replace `<new_password>` with the new TPM password, by following the recommendations in the section TPM administration password.

If you have forgotten the TPM password, refer to the section Troubleshooting.

Sealing the TPM

The TPM has to be sealed in the following cases:

- When the TPM can no longer be accessed,
- When a new TPM sealing policy is available and you wish to apply it.

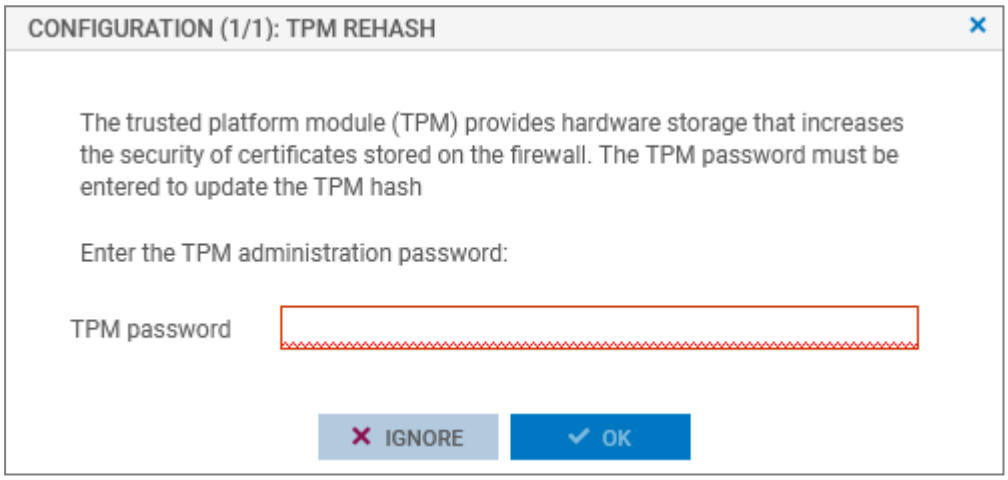
The status of the TPM is key to identifying whether the TPM needs to be resealed. When the TPM is sealed, PCR hash values are recalculated.

From the web administration interface

This use case is exclusive to SNS 4.8.7 and higher versions.

IMPORTANT
As a reminder, the integrity of the SNS firewall and its TPM will be compromised if Secure Boot is not enabled. As such, you are advised to enable it before resealing the TPM.

1. Log in to the SNS firewall web administration interface.
   A window automatically appears when the TPM needs to be sealed. In a high availability configuration, a window also appears if the TPM on the passive firewall needs to be sealed. If both members of the cluster are concerned, two windows will appear one after the other.



2. Enter the TPM password in the relevant field.
3. Click on **OK**.

From the CLI console

1. Seal the TPM on the SNS firewall with the command:
   ```
   SYSTEM TPM PCRSEAL tpmpassword=<password>
   ```
   Replace `<password>` with the TPM password.
2. If the SNS firewall is part of a high availability cluster, seal the TPM on the passive firewall with the command:
   ```
   SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive
   ```

From the SSH console

SSH access must be allowed on the firewall. Only the *admin* account can perform this operation.

Seal the TPM on the SNS firewall with the command:

```
tpmctl -svp <tpmpassword>
```

Replace `<password>` with the TPM password.

Disabling the TPM

From a CLI console, disable the TPM using the command:

```
SYSTEM TPM RESET tpmpassword=<password> force=<on|off>
```

- Replace `<password>` with the TPM password,
- Enter `force=on` if private keys in certificates are protected by the TPM, and you wish to disable it by force anyway. The protected private keys will then be decrypted.

Managing protection on private keys in SNS firewall certificates

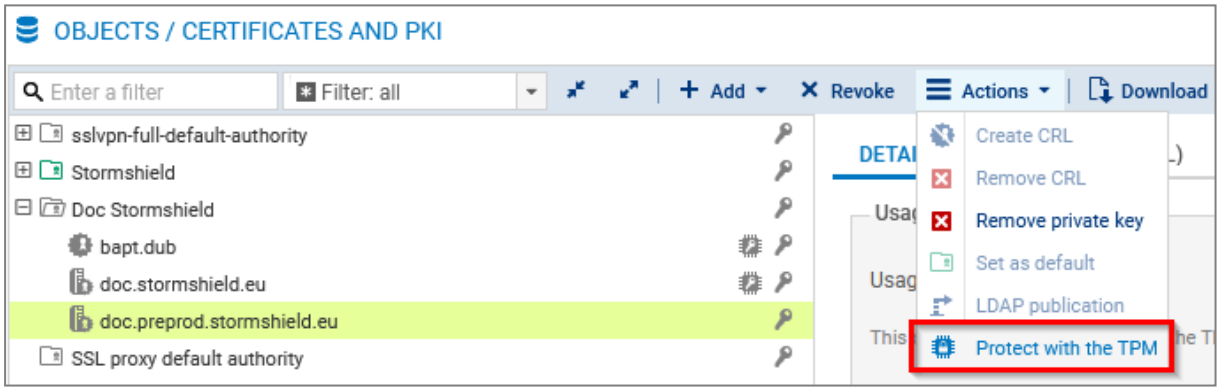
This section explains how to protect the private keys of certificates on an SNS firewall using the TPM, and how to check whether a private key is protected.

Managing protection on private keys in a certificate that already exists

From the web administration interface

This use case is exclusive to SNS 4.8.7 and higher versions.

1. Go to **Configuration > Objects > Certificates and PKI**.
2. Select the certificate (identity) in question.
3. To protect the private key of the certificate, click on **Actions > Protect with the TPM.** To remove its protection, refer to the section **From the CLI console**.
4. Click on **OK**.



From the CLI console

1. Show certification authorities with the command:

   ```
   PKI CA LIST
   ```

   If required, you can show the list of intermediate certification authorities that were signed by the root authority in question, by adding `CANAME=<RootCA>` in the command.
2. Show the certificates issued by the certification authority (`<CA>`) with the command:

   ```
   PKI CERT LIST CANAME=<CA>
   ```
3. Depending on what you wish to do with the certificate (`<CERTNAME>`) in question:
   - To protect its private key, run the command:

     ```
     PKI CERT PROTECT CANAME=<CA> NAME=<CERTNAME> tpm=ondisk
     ```
   - To remove its protection, run the command:

     ```
     PKI CERT PROTECT CANAME=<CA> NAME=<CERTNAME> tpm=none
     tpmpassword=<password>
     ```

     Replace `<password>` with the TPM password.
4. Activate the new configuration with the command:

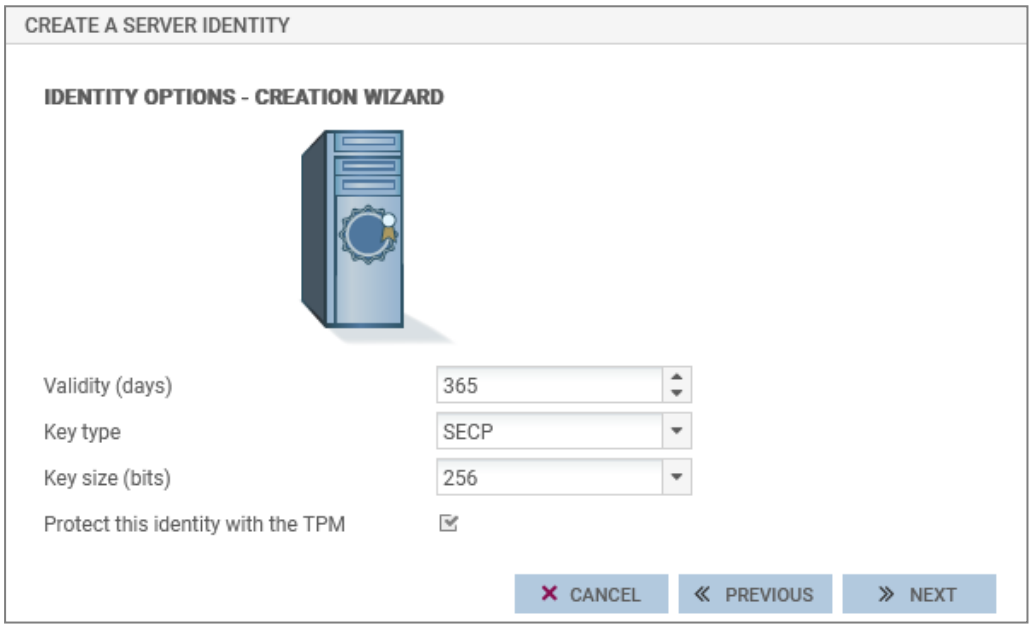
   ```
   PKI ACTIVATE
   ```

Adding a certificate and protecting its private key

From the web administration interface

1. Go to **Configuration > Objects > Certificates and PKI**.
2. Click on **Add** and select the certificate (identity) in question.
3. Fill out the requested information. Select the **Protect this identity with the TPM** checkbox throughout the steps.
4. Click on **Finish**.

For more information, refer to the section on **Certificates and PKI** in the *SNS* v4.8 or v4.3 LTSB *user guide*, depending on the version used.



From the CLI console

1. Add a new certificate with the command:

   ```
   PKI CERT CREATE
   ```

   Use the token `tpm=ondisk` to protect the private key of the certificate.

   If required, show command help with:

   ```
   PKI CERT CREATE HELP
   ```

2. Activate the new configuration with the command:

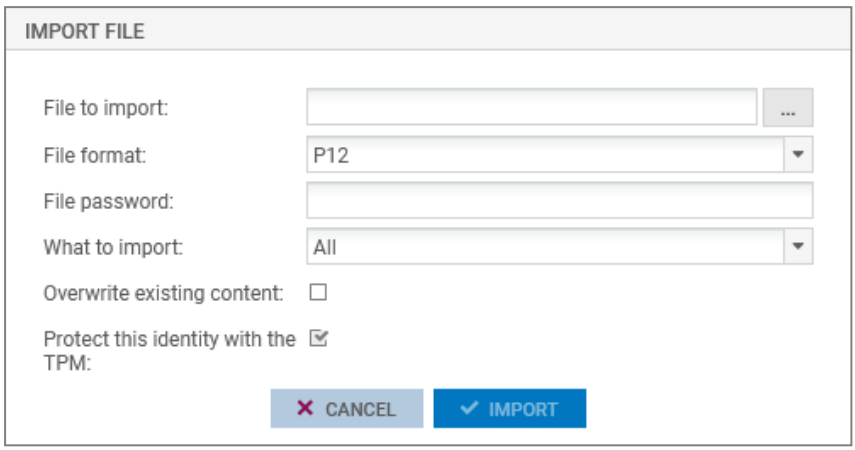
   ```
   PKI ACTIVATE
   ```

Importing a certificate and protecting its private key

From the web administration interface

1. Go to **Configuration > Objects > Certificates and PKI**.
2. Click on **Add > Import a file**.
3. Fill out the requested information. Select the **Protect this identity with the TPM** checkbox throughout the steps.
4. Click on **Finish**.

For more information, refer to the section on **Certificates and PKI** in the *SNS* v4.8 or v4.3 LTSB *user guide*, depending on the version used.



From the CLI console

1. Import a certificate by using the command:

```
PKI IMPORT type=<req|cert|pkey|crl|ca|all> format=<p12|pem|der>
password=<pass> force=<0|1> tpm=ondisk < /tmp/myfile.p12
```

   - Customize the configuration tokens,
   - In the example above, the file *myfile.p12*, uploaded to the SNS firewall earlier in the */tpm/* directory, will be imported.

   If required, show command help with:

```
PKI IMPORT HELP
```

2. Activate the new configuration with the command:

```
PKI ACTIVATE
```

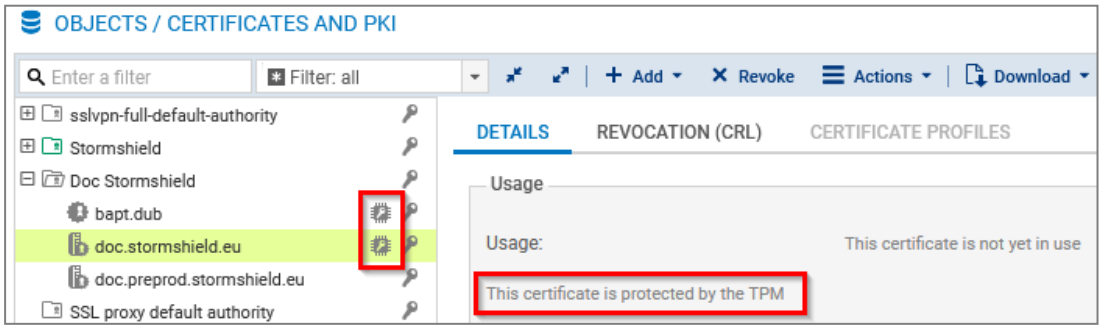
Checking whether the private key of a certificate is protected

From the web administration interface

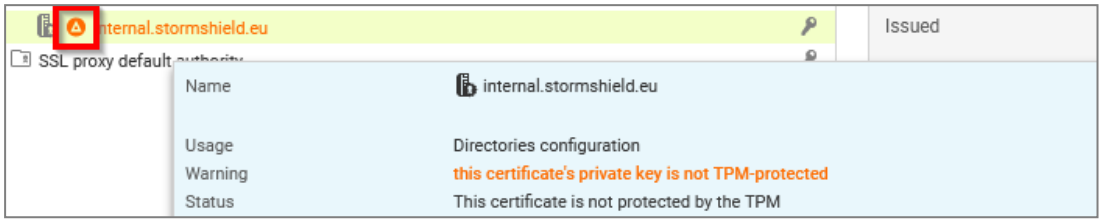
This use case is exclusive to SNS 4.8.7 and higher versions.

Go to **Configuration > Objects > Certificates and PKI**.

- The icon indicates that the private key of the certificate is protected by the TPM. This information is also available in the **Details** tab of the certificate, and in the tooltip that appears when scrolling over the certificate.



- The icon indicates that the certificate is used in the SNS firewall configuration, but its private key is not protected by the TPM. This information is also available in the tooltip that appears when scrolling over the certificate.



From the CLI console

- To verify the certificates that are currently being used in the SNS firewall configuration, run the command:

```
MONITOR CERT
```

In the result, `tpm=Used` indicates that the private key is protected by the TPM.

- To verify a particular certificate, run the command:

```
PKI CERT SHOW CANAME=<CA> NAME=<CERTNAME>
```

In the result, `tpm=ondisk` indicates that the private key is protected by the TPM.

- To verify the certificates of a certification authority on an SNS firewall:
  1. Show certification authorities with the command:

     ```
     PKI CA LIST
     ```

     If required, you can show the list of intermediate certification authorities that were signed by the root authority in question, by adding `CANAME=<RootCA>` in the command.
  2. Show the certificates issued by the certification authority (`<CA>`) with the command:

     ```
     PKI CERT LIST CANAME=<CA>
     ```

     In the result, `tpm=ondisk` indicates that the private key is protected by the TPM.

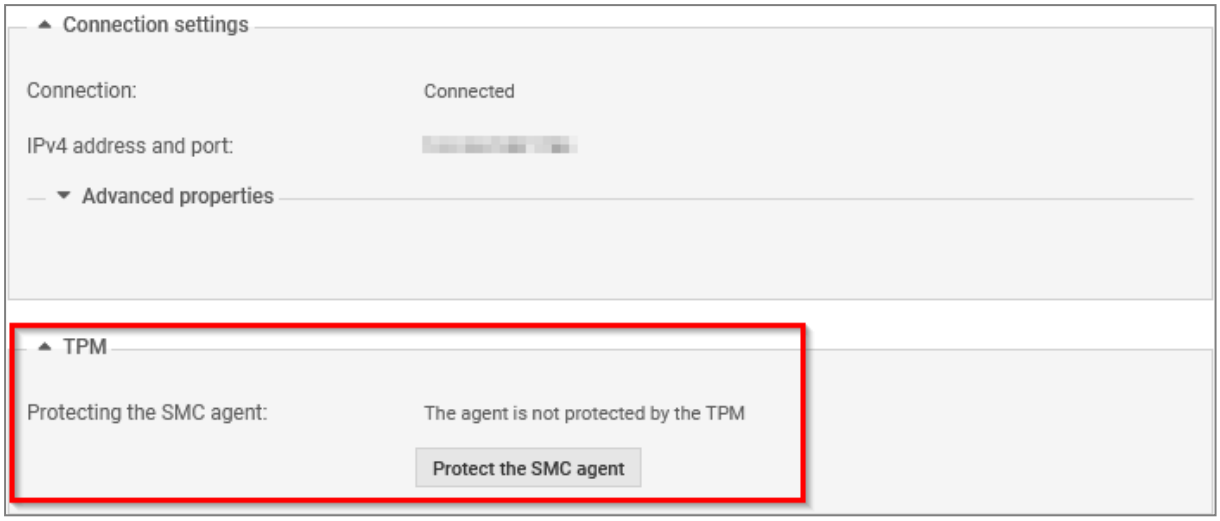
Firewall pools managed by an SMC server

Managing protection on the private key of the certificate that is used to communicate with the SMC server

This use case is exclusive to SNS 4.8.7 and higher versions.

1. Go to **Configuration > System > Management Center.**
2. In the **TPM** section, to protect the private key of the certificate that is used to communicate with the SMC server, click on **Protect the SMC agent**. To remove its protection, click on **Unprotect the SMC agent**.
3. Confirm changes.

IMPORTANT
If the private key of the certificate that is used to communicate with the SMC server is protected and access to the TPM is denied in the future, communications with the SMC server will no longer be possible until the TPM has been resealed. In the meantime, the SNS firewall can no longer be managed through the SMC server.



These operations can also be performed from the CLI console using these commands:

- To protect the private key of the certificate:
  ```
  CONFIG FWADMIN PROTECT tpm=ondisk
  ```
- To remove protection on the certificate's private key:
  ```
  CONFIG FWADMIN PROTECT tpm=none tpmpassword=<password>
  ```
  Replace `<password>` with the SNS firewall's TPM password.

You can run these commands on a pool of SNS firewalls from the SMC server. For more information, refer to the section Running SNS CLI commands on a pool of firewalls in the *SMC administration guide*.

Managing protection on the private key of the SNS firewall's certificates from the SMC server

For more information on protecting the private key in SNS firewall certificates from the SMC server, refer to the following sections of the *SMC administration guide*:

- Enabling TPM protection on existing private keys,
- Importing or declaring a certificate for a firewall,
- Finding out whether a private key is TPM-protected.

NOTE
When the TPM is initialized, the private key in certificates that the SMC server declared on the SNS firewall are protected by the TPM by default. To change this setting, refer to the section Disabling TPM private key protection in the *SMC administration guide*.

Using certificates with TPM-protected private keys

This section explains how to use certificates with TPM-protected private keys in the configuration of an SNS firewall.

SSL/TLS decryption (web administration interface and captive portal)

This use case is exclusive to SNS 4.8.7 and higher versions.

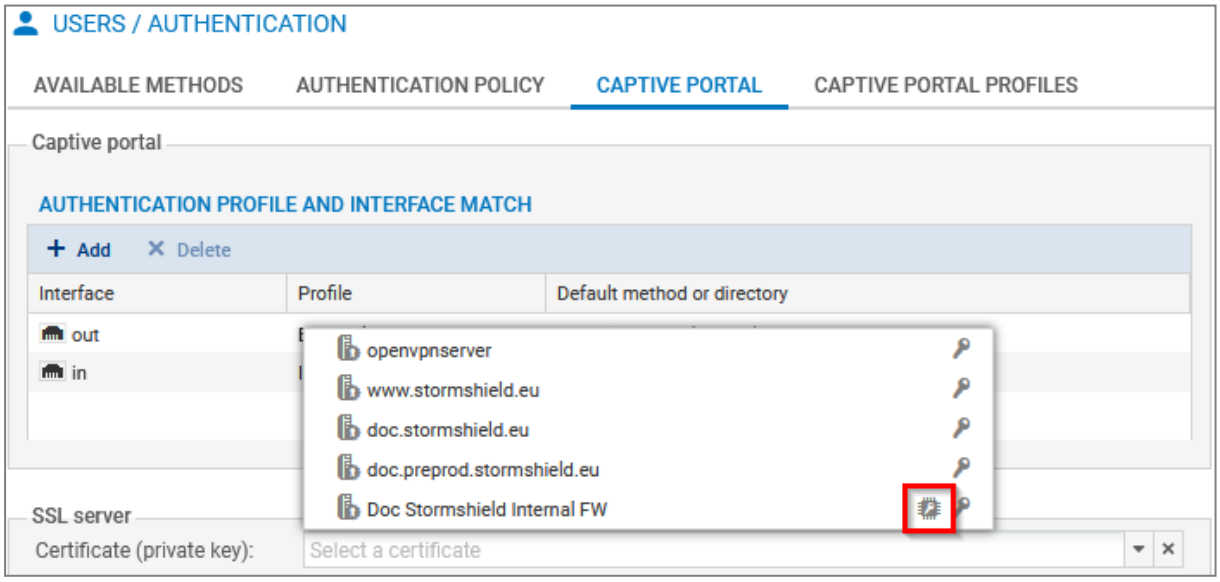
The private key in the certificate presented by the web administration interface and the SNS firewall's captive portal can be protected by the TPM.

To check/change the certificate used:

1. Go to **Configuration > Users > Authentication**, **Captive portal** tab, **SSL server** section.
2. In the **Certificate (private key)** field, select the desired certificate. The icon indicates certificates with a TPM-protected private key.
3. Apply changes.
   The connection to the web administration interface will be lost. A warning message may appear when you go back to the authentication page. You can proceed to the website.

NOTE
A backup certificate can be used to maintain access to the web administration interface if the private key of the selected certificate is protected, and access to the TPM is denied.

- On SNS 4.8.7 and higher versions of 4.8.x in factory configuration, this is a certificate that corresponds to the SNS firewall's serial number,
- On versions 5 in factory configuration, the certificate is self-generated for this access.



SSL VPN

This use case is exclusive to SNS 4.8.7 and higher versions.

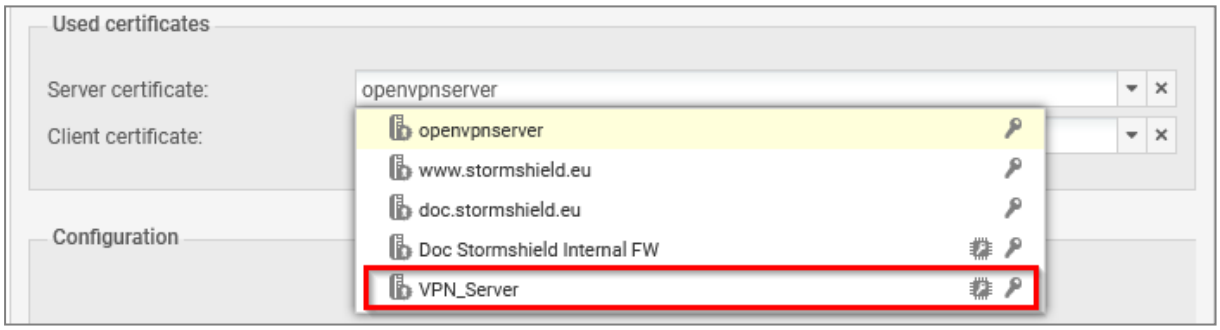
The private key of the certificate that is presented by the SNS firewall SSL VPN service can be protected by the TPM.

IMPORTANT
If the private key of the selected certificate is protected, and access to the TPM is denied in the future, you will no longer be able to set up SSL VPN tunnels with the SNS firewall until the TPM has been resealed.

To check/change the certificate used:

1. Go to **Configuration > VPN > SSL VPN**, **Advanced properties** area, **Certificates** section.
2. In the **Server certificate** field, select the desired certificate. The icon indicates certificates with a TPM-protected private key. The selected certificate must be issued from the same certification authority as the one for the client certificate.
3. In the **Client certificate** field, you cannot select certificates that have TPM-protected private keys. This is because the private keys of such certificates must be available in plaintext (unencrypted) in the VPN configuration that is distributed to VPN clients.
4. Apply changes.

   If you are using the Stormshield VPN SSL client in automatic mode, the VPN configuration will automatically be retrieved at the next connection. For all other use cases, the VPN configuration must be imported again (*.ovpn* file). For more information, refer to the technical note Configuring and using the SSL VPN on SNS firewalls.



IPsec VPN

The private key of the certificate that is presented to set up IPsec tunnels in a certificate authentication can be protected by the TPM.

IMPORTANT
If the private key of the selected certificate is protected, and access to the TPM is denied in the future, you will no longer be able to set up IPsec VPN tunnels with the SNS firewall until the TPM has been resealed.

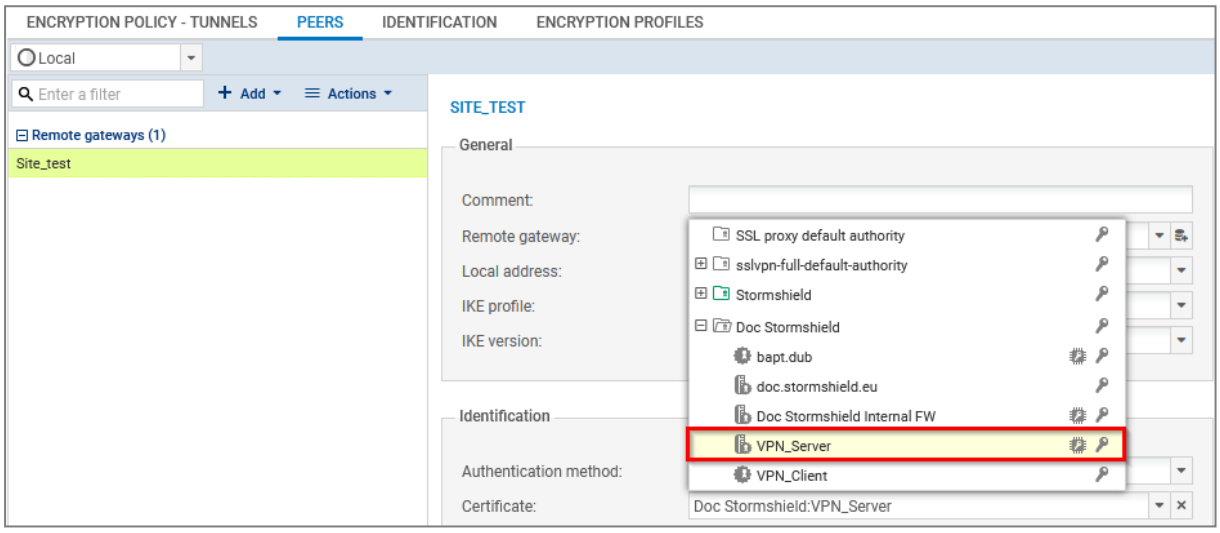
To check/change the certificate used:

1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. In the grid, select the peer that was used in the VPN configuration.

3. In the **Identification** section, **Certificate** field, select the desired certificate. The icon indicates certificates with a TPM-protected private key.

> **NOTE**
> In configurations using the IPsec IKEv1 VPN tunnel manager, do not choose a certificate with a protected private key, as tunnels will no longer be able to set up.

4. Apply changes.



Communications with the SMC server

This use case is exclusive to SNS 4.8.7 and higher versions.

The private key of the certificate that is used to communicate with the SMC server can be protected by the TPM.

> **IMPORTANT**
> As a reminder, if the private key of the certificate that is used to communicate with the SMC server is protected and access to the TPM is denied in the future, communications with the SMC server will no longer be possible until the TPM has been resealed.

For more information, see the section Firewall pools managed by an SMC server.

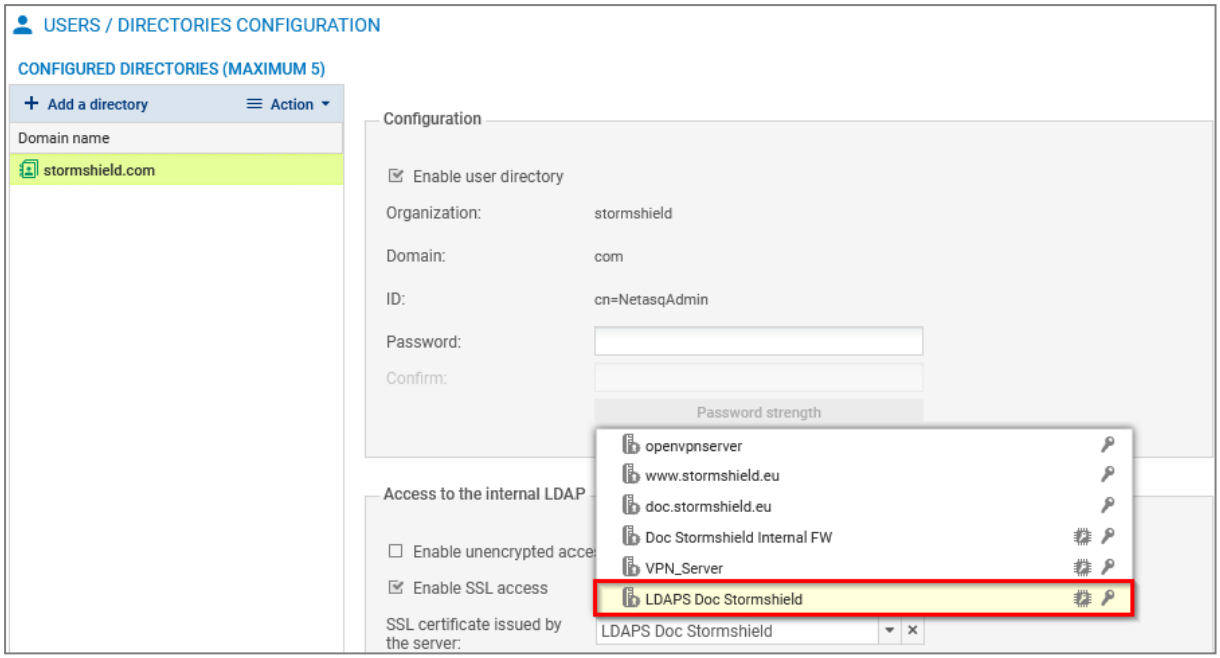
Internal LDAP

This use case is exclusive to SNS 4.8.7 and higher versions.

The private key of the certificate that is used for authentication to the internal LDAP directory can be protected by the TPM.

To check/change the certificate used:

1. Go to **Configuration > Users** > **Directory configuration**.
2. Select the internal LDAP directory from the grid.
3. In **Access to the internal LDAP, SSL certificate issued by the server** field, select the desired certificate. The icon indicates certificates with a TPM-protected private key.
4. Apply changes.



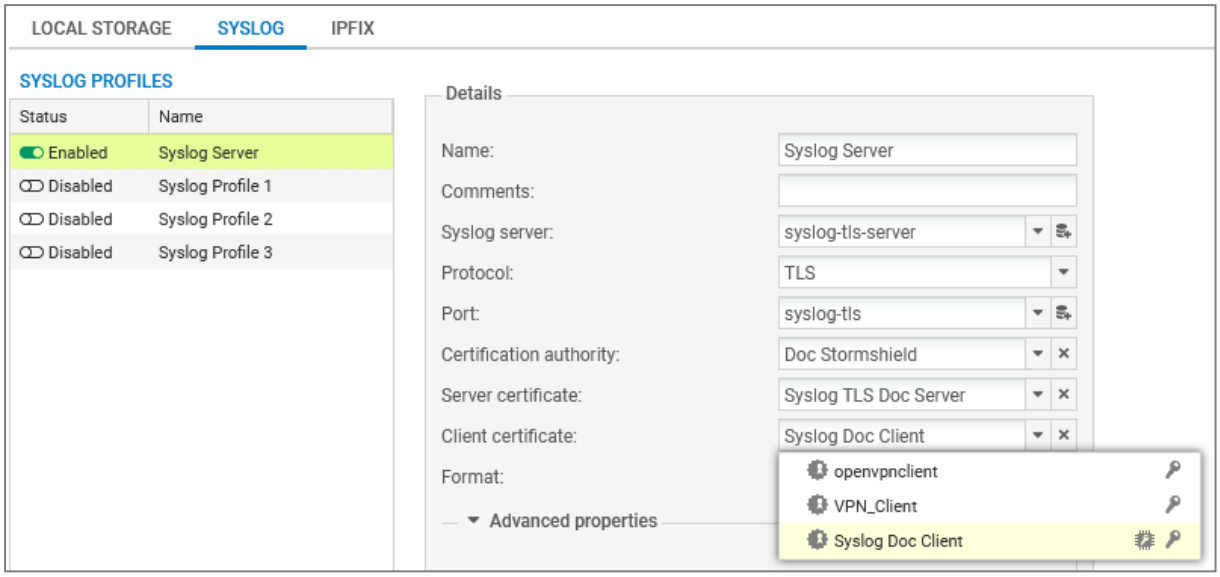
Sending logs to a TLS syslog server

This use case is exclusive to SNS 4.8.7 and higher versions.

The private key of the certificate that is presented by the SNS firewall to authenticate on the Syslog server can be protected by the TPM.

To check/change the certificate used:

1. Go to **Configuration > Notifications > Logs – Syslog - IPFIX, Syslog** tab.
2. Select the profile of the syslog server that you wish to modify from the grid. The details of the profile appear on the right.
3. In the **Certification authority** field, select the certification authority (CA) that signed the certificates that the SNS firewall and Syslog server will present in order to authenticate mutually.
4. In the **Server certificate** field, select the certificate that the Syslog server will need to present in order to authenticate on the SNS firewall. You cannot select a certificate with a TPM-protected private key.
5. In the **Client certificate** field, select the certificate that the SNS firewall will need to present in order to authenticate on the Syslog server. The icon indicates certificates with a TPM-protected private key.
6. Apply changes.
7. Ensure that the syslog server has the selected client certificate. You can export the certificate as a P12 file in **Configuration > Objects > Certificates and PKI**.


LOCAL STORAGE
SYSLOG
IPFIX
SYSLOG PROFILES
Status
Name
Enabled
Syslog Server
Disabled
Syslog Profile 1
Disabled
Syslog Profile 2
Disabled
Syslog Profile 3
Details
Name:
Syslog Server
Comments:
Syslog server:
syslog-tls-server
Protocol:
TLS
Port:
syslog-tls
Certification authority:
Doc Stormshield
Server certificate:
Syslog TLS Doc Server
Client certificate:
Syslog Doc Client
Format:
Advanced properties
openvpnclient
VPN_Client
Syslog Doc Client

Explanations on usage when the TPM is initialized

This section explains how to back up and restore a configuration, how to set up the initial configuration using a USB key, and how to calculate the high availability quality factor once the TPM has been initialized.

Backing up a configuration

The configuration of the SNS firewall can be manually or automatically backed up from the web administration interface, the CLI console, or from the SMC server.

Depending on the method used, there are specific conditions on the presence of protected private keys in the backup file, and on their encryption status.

Manual backups			Automatic backups	
SNS interface	SNS CLI console	SMC (CLI script)	SNS interface	SMC interface
✅ Includes private keys (may or may not be TPM-protected)				❌ Excludes private keys
Protected private keys are decrypted	Protected private keys are decrypted They can be kept encrypted with the token *ondiskprotect=1*		Protected private keys remain encrypted	N/A

For more information on backing up a configuration:

- For the SNS firewall web administration interface, go to **Maintenance** > **Backup** tab in the v4.8 or v4.3 LTSB *SNS User guide*, depending on the version used.
- For the SNS firewall CLI console, by using the `CONFIG BACKUP` command:
```
CONFIG BACKUP HELP
```
- For the SMC server, go to Backing up the configuration of firewalls in the *SMC administration guide.*

> **IMPORTANT**
> The SMC server makes it possible to automatically back up the configuration on SNS firewalls. When the TPM is initialized, **all** private keys of certificates, regardless of whether they are TPM-protected, will be **excluded** from automatic backups.

Restoring a configuration backup

Backups containing encrypted private keys can **only** be restored on the original firewall. Encrypted private keys cannot be decrypted on another SNS firewall as the symmetric key is assumed to be different.

There are a few exceptions in the following cases:

- If the symmetric key derivation mechanism was used to generate the symmetric key from the TPM password, and this password is the same on both SNS firewalls. In this case, the symmetric key is the same on both SNSfirewalls.

- Following the exchange of a firewall (RMA) configured in high availability. For more information, refer to the instructions in the Stormshield knowledge base article **Following an RMA, how can I synchronize the configuration and the content of the TPM?** (authentication required).

Initial configuration via USB key

During the initial configuration of an SNS firewall via USB key, two operations allow you to interact with the TPM:

- The **initTPM operation** allows you to initialize the SNS firewall's TPM. If the SNS firewall is part of a high availability cluster, the **mechanism that derives the symmetric key** will automatically be used.
- The **p12import operation** allows you to import PKCS#12 files in *.p12* format and protect the private key contained in the file with the TPM. The *initTPM* operation must be carried before the *p12import* operation.

For more information on implementing this procedure and other possible operations, refer to the technical note **Initial configuration via USB key**.

Calculating the high availability (HA) quality factor

The status of the TPM can be applied to the calculation of the high availability (HA) quality factor.

The configuration token `TPMQualityIncluded=1` found in the *[Global]* section of the configuration file *ConfigFiles/HA/highavailability* indicates that the status of the TPM has been applied.

On SNS versions 4.8.7 and higher, the status of the TPM will not be taken into account when calculating the high availability quality factor if Secure Boot is disabled.

IMPORTANT
As a reminder, the integrity of the SNS firewall and its TPM will be compromised if **Secure Boot** is not enabled.

For more information on calculating the high availability (HA) quality factor, refer to the technical note **High availability on SNS**.

Troubleshooting

This section lists several issues that are frequently encountered when the TPM is used. If the issue you encounter cannot be found in this list, we recommend that you refer to the Stormshield knowledge base.

TIP
To troubleshoot the TPM, run this command in an SSH console:

```
tpmctl -a -v
```

SSH access must be allowed on the SNS firewall.

Lost TPM administration password

Situation: The TPM password is required to perform operations, but the password was lost.

Cause: The password was not kept or saved in a secure location.

Solution: You will not be able to reset the TPM password, and Stormshield is not in a position to recover it.

As a last resort, if you cannot remember it, you can reinitialize the TPM by following the instructions in the Stormshield knowledge base article I have lost my TPM password, how can I reset it? (authentication required).

IMPORTANT
By resetting the TPM, you will **not be able** to recover the private keys that it protects. You will need to import the certificates in question again, and protect their private key.

Accessing the SNS firewall web administration interface and backup certificate

Situation: It is still possible to access the web administration interface on an SNS firewall in version 4.8.7 or higher, which has a TPM-protected private key from the certificate presented by the web administration interface, even though the TPM status indicates that it has to be resealed.

Cause: The technical characteristics of the system have been modified. As such, the TPM can no longer be accessed because the hash values of PCRs have changed, preventing the decryption of the protected private key from the certificate presented by the web administration interface.

However, a backup certificate can be used to maintain the access to the web administration interface:

- On SNS 4.8.7 and higher versions of 4.8.x, this is the default certificate in the factory configuration, which corresponds to the SNS firewall's serial number,
- On SNS version 5 in factory configuration, the certificate is self-generated for this access.

Solution: Although to the web administration interface can still be accessed through the backup certificate, all private keys protected by the TPM can no longer be decrypted. To fix this issue, first check that the changes to the technical specifications are legitimate, then seal the TPM by following the procedure Sealing the TPM.

Some features no longer function

After updating the SNS firewall software

Situation: After the software on an SNS firewall or SNS firewall cluster is updated to version 4.3 LTSB or higher, features that use certificates with a protected private key no longer function.

Cause: The system's technical characteristics have been modified following the update of the SNS firewall. As such, the TPM can no longer be accessed because the hash values of PCRs have changed, preventing the decryption of protected private keys. The TPM status indicates that it has to be resealed.

Solution: Seal the TPM by following the Sealing the TPM procedure.

After inserting a storage medium and restarting the SNS firewall

Situation: After inserting a storage medium and restarting the SNS firewall, features that use certificates with a protected private key no longer function.

Cause: The system's technical characteristics were modified when the SNS firewall started, as a new storage medium was detected. As such, the TPM can no longer be accessed because the hash values of PCRs have changed, preventing the decryption of protected private keys. The TPM status indicates that it has to be resealed.

Solution: If the storage medium has a legitimate reason for being used, seal the TPM by following the Sealing the TPM procedure.

After the passive firewall switches to active (high availability)

Situation: After a passive firewall switches to active, features that use certificates with a protected private key no longer function.

- *Cause 1*: The mechanism that derives the symmetric key was not enabled on the SNS firewall cluster. You can check its status by running this CLI command:

  ```
  SYSTEM TPM STATUS tpmpassword=<password>
  ```

  Solution: Enable the symmetric key derivation mechanism on the cluster and renew the symmetric key by running the following CLI commands:

  ```
  SYSTEM TPM RENEW tpmpassword=<password> derivekey=on
  HA TPMSYNC tpmpassword=<password>
  ```

  - Replace `<password>` with the TPM password,
  - As the firewall is part of a high availability cluster, enter `derivekey=on`.
- *Cause 2*: Both SNS firewalls in the cluster were recently updated to SNS version 4.3 LTSB or higher. After the switch, the TPM can no longer be accessed because the hash values of PCRs have changed, preventing the decryption of protected private keys. The TPM status indicates that it has to be resealed.

  Solution: Seal the TPM by following the Sealing the TPM procedure.

Further reading

Additional information and answers to some of your questions may be found in the Stormshield knowledge base (authentication required).

To update the TPM version on an SNS firewall, refer to the technical note Updating the TPM version on SNS firewalls.

Appendix: points to note when updating SNS firewalls on which the TPM has been initialized

This section provides important points to note when updating SNS firewalls on which the TPM has been initialized.

Context

If there is any indication in the *SNS Release Notes* that the TPM will need to be resealed following an update, we strongly recommend that you read the information in this section before updating the SNS firewall.

Depending on the changes made to the new SNS version, PCR hash values may change after the update, and access to the TPM may then be denied.

If access to the TPM is denied, SNS firewall features that use certificates with protected private keys will no longer function after the update, as long as access to the TPM has not been restored. For example, you may no longer be able to set up VPN tunnels with the SNS firewall, or manage it through an SMC server.

For more information on PCRs and access to the TPM, see the section Platform configuration registers.

Incremental versions to apply

This table summarizes the incremental versions that need to be taken into account when **updating to version 4.8 or higher from the latest available 4.3 LTSB version**. When a version is skipped, the contents of intermediate versions apply.

Version	Description
4.8.0	Access to the TPM denied. Reseal the TPM.
4.8.3	Access to the TPM denied. Reseal the TPM.
4.8.7	If certificates with a protected private key are used for VPN SSL and IPsec services, reseal the TPM. This issue has been fixed in version 4.8.9. Access to the TPM still possible, but its sealing policy has changed. • Reseal the TPM to benefit from the new sealing policy. When you log in to the SNS firewall web administration interface, a window will ask you to do so. • With the new sealing policy, the integrity of the SNS firewall and its TPM will be compromised if Secure Boot is not enabled. As such, you are advised to enable it before resealing the TPM.
As of version 4.8.9	Update blocked if these three conditions are combined: • The SNS firewall is managed by an SMC server, • The private key of the certificate that is used to communicate with the SMC server is protected, • The TPM sealing policy will be changed when the update is complete.

Recommendations to follow when updating SNS firewalls on which the TPM has been initialized

1. If you are unsure whether the TPM has been initialized on your SNS firewall, refer to the section Checking the status of the TPM.
2. Check whether the version that you wish to install requires the TPM to be resealed. To do so, refer to the section *Incremental versions to apply* and information provided in *SNS Release Notes*.
3. If the TPM is initialized and needs to be sealed after the update, check that the private key of the certificate that is used to communicate with the SMC server, or that of the certificate presented by the SNS firewall's VPN services, **is not protected**. For the SMC server, see the section Firewall pools managed by an SMC server. For VPN services, see the section Using certificates with TPM-protected private keys.
4. If the private key in these certificates is protected, remove this protection **before** updating the SNS firewall. For the SMC server, see the section Firewall pools managed by an SMC server. For VPN services, see the section Managing protection on private keys in a certificate that already exists.
5. Once these private keys are no longer protected, the SNS firewall can be updated.
6. Once the SNS firewall is updated, reseal the TPM. When you log in to the SNS firewall web administration interface, a window will ask you to do so. Refer to the Sealing the TPM whenever necessary.
7. Once the TPM has been sealed, private keys on which protection was removed earlier can be protected again. For the SMC server, see the section Firewall pools managed by an SMC server. For VPN services, see the section Managing protection on private keys in a certificate that already exists.

documentation@stormshield.eu